

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

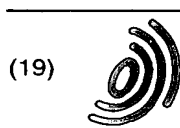
- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problems Mailbox.**

THIS PAGE BLANK (USPTO)

BG



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11) EP 0 779 570 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
18.06.1997 Bulletin 1997/25

(51) Int Cl.⁶ G06F 1/00

(21) Application number: 96308205.2

(22) Date of filing: 13.11.1996

(84) Designated Contracting States:
DE FR GB

• Peebles, Thomas Frank
Austin, Texas 78758 (US)

(30) Priority: 11.12.1995 US 570463

(74) Representative: Zerbi, Guido Maria
Intellectual Property Department,
IBM United Kingdom Ltd.,
Hursley Park
Winchester, Hampshire SO21 2JN (GB)

(71) Applicant: International Business Machines
Corporation
Armonk, N.Y. 10504 (US)

(72) Inventors:
• Kells, Timothy Roger
Round Rock, Texas 78681 (US)

(54) System and method for supporting distributed computing mechanisms in a local area network server environment

(57) LAN server machines are configured to utilize their existing mechanisms to pass generic security sub-system (GSS) distributed computing environment (DCE) credentials. The server management block (SMB) protocol is extended to facilitate exchange of such credentials wherein the server utilizes the GSS API interface to obtain and validate such credentials. The GSS interface provides tokens which encapsulate all necessary information to perform mutual authentication between the client and server.

A new protocol level is defined with respect to such SMB protocol extensions which includes a new protocol name exchanged in the negotiate protocol (NP) SMB. Pre-existing LAN servers will turn on a bit in the SMB_Secmode field in the NP response indicating that the server supports exchange of secpkgX SMB. The server will then wait for an SMB secpkgX or SMB sess-setupX response. The former response will permit the user/client and server to exchange GSS tokens utilizing a conventional LAN server mechanism and to thereby and mutually authenticate.

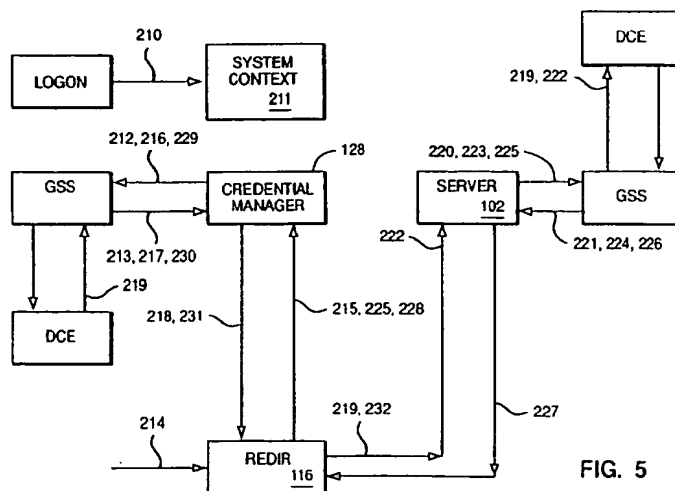


FIG. 5

DescriptionTechnical Field

5 This invention relates to authentication in computer systems and, more particularly, to authentication techniques in client-server local area network environments.

Background of the Invention

10 In a session setup of a typical local area network, a process transpires conventionally wherein, with reference to Fig. 2, a client-user 100 and a server 102 negotiate a network protocol 104 (NP). During such negotiation, a protocol and associated protocol level 208 are agreed upon (corresponding, for example, to CORE, LAN 2.1, etc.) whereupon a session key 106 is determined for the client 100.

15 The client-user 100 will typically transmit information such as the user's id, name, and password 112 to the server 102 and, more particularly, to a redirector 116, Fig. 8 which serves as the network interface to and from the LAN server 102. The redirector 116 essentially serves the purpose of a network interface, redirecting disk drives and file input/output, etc. For example, if a client connects to a drive, to the client it may appear to be a local drive. However, the redirector essentially serves as a file system which may pass the drive specification to the actual file system which will manage the drive, thereby redirecting requests from the client to the actual file server handling the drive, such process
20 being transparent to the client.

In conventional operation, the server 102 then would typically examine its database 118, Fig. 3, and based upon the user id, would extract the user's password and session key 106, Fig. 2, and determine if there was a match. If so, the server 102 would then fetch the user definition 120, Fig. 3 out of the server's local database 118. It will be noted that this session key 106 is essentially a timestamp or serial number. In the implementation under consideration, for
25 reasons which will become apparent in discussion of the invention, rather than employing the database 118, the implementation employs the Distributed Computing Environment (DCE) and associated Kerberos registry 122, Fig. 4, and more particularly, the directory and security server (DSS) component of DCE wherein the user definition resides.

Thus in summary, at logon, a client 100, when logging onto a distributed computing environment negotiates a protocol 104, Fig. 2, which results in a protocol level 208 being returned. It is desirable in some local area network server environments such as the LAN Server Enterprise (LSE) product of the IBM Corporation to employ DCE to
30 authenticate use with DCE and thus to associate DCE credentials for users that connect to the LAN because it is deemed to be a relatively more secure environment than that effected by a typical LAN server authentication mechanism. Thus it is desirable at logon to obtain DCE credentials which the server 102 may understand, such DCE credentials being normally obtained through remote procedure calls (RPC).

35 It has been found, however, that a problem may arise in such local area networks wherein no mechanism is provided to obtain such DCE credentials from the client 100 to the server 102. More particularly, in the case of the LSE and similar LAN products, for example, RPC calls are not utilized natively but nevertheless the server needs to obtain genuine credentials to authenticate the user during the session setup. Such credentials are utilized in determining access to LSE resources which are protected by POSIX access controls lists (ACLs). Thus, a serious problem was
40 presented of providing a mechanism to obtain such DCE credentials from the client to the server with current protocols such as those typically defined by the X/Open Association as represented by the Server Management Block (SMB) protocols, for example, while nevertheless utilizing conventional LAN server mechanisms.

It is an object of the present invention to provide a technique which alleviates the above drawbacks.

45 Summary of the Invention

According to the present invention we provide a method for improving mutual authentication during session setup with (DCE) credentials between clients and servers interconnected in a LAN server environment which does not support remote procedure calls (RPC) natively, comprising: predefining an extension of a server management block (SMB)
50 protocol to exchange credentials; accessing with said server as a function of said predefined extension a generic security subsystem (GSS) through a GSS API interface defined by said DCE; and obtaining and validating said credentials from said GSS in response to said accessing.

Further according to the present invention we provide an apparatus for improving mutual authentication during session setup with distributed computing environment (DCE) credentials between clients and servers interconnected
55 in a LAN server environment which does not support remote procedure calls (RPC) natively, comprising: means for predefining an extension of a server management block (SMB) protocol to exchange credentials; means for accessing with said server as a function of said predefined extension a generic security subsystem (GSS) through a GSS API interface defined by said DCE; and means for obtaining and validating said credentials from said GSS in response to

said accessing.

In a preferred embodiment of the invention, LAN server machines in a computerized LAN network are configured so as to permit them to utilize their existing mechanisms to pass generic security subsystem (GSS) distributed computing environment (DCE) credentials. The server management block (SMB) protocol defined by X/Open is extended to facilitate exchange of such credentials wherein the server utilizes the GSS API interface provided by DCE to obtain and validate such credentials. The GSS interface provides tokens which encapsulate all necessary information to perform mutual authentication between the client and server.

In the preferred embodiment, with respect to such SMB protocol extensions, a new protocol level is defined which, in the specific embodiment includes a new protocol name exchanged in the negotiate protocol (NP) SMB. Pre-existing LAN servers such as the IBM Lan Server Enterprise (LSE) product will turn on a bit (bit 2 with respect to LSE) of the SMB_secmode field in the response, such bit indicating that the server supports exchange of secpkgX SMBs. The server will then wait for an SMBsecpkgX or SMBsesssetupX request. The former response will permit the user/client and server to exchange GSS tokens and mutually authenticate and will further allow the server to select from multiple packages. The pre-existing LAN server product will define a new package under an SMB_pkgname which the LAN server will send and recognize in order to handle a GSSDCE token. A user on a client will be authenticated once the SMBsecpkgX has flowed because the authentication will allocate and return the necessary data structures in order for the server to track the user.

Further in accordance with a preferred embodiment of the invention, as to processing GSS tokens, on the client side, a gss_initiate_sec_context function is called in order for the client to obtain a token to send to the server. The token is sent to the server and a return token then received from the server. The return token is then passed to a gss_initiate_sec_context function, which will now return whether or not the server is authenticated. If the server is not authenticated, session establishment is terminated.

On the server side, when the SMBsecpkgX response is received, the token is extracted and processed by a gss_accept_sec_context function. If the client is authenticated, a token to send to the client is also received. The token is sent to the client on the SMBsecpkgX response. After sending the SMB, the server extracts the user's credentials from the GSS token. The credentials are attached to the session data structures and are utilized thereafter whenever the user attempts to access resources.

Regarding the redirector-GSS interface, in a preferred embodiment herein disclosed, the LAN server redirector normally runs at ring 0 whereas the GSS runs at ring 3, meaning that the redirector and GSS may not communicate directly. Accordingly, in accordance with a preferred embodiment of the invention, a credential manager process is created as an intermediary. The credential manager gives a captive thread to the redirector at startup. As connections are made to the LAN servers, the redirector utilizes the captive threads to request and process GSS tokens. The credential manager uses the credentials of the user currently logged onto the LAN server to obtain the tokens. A user profile management (UPM) process notifies the credential manager of logon and logoff events. This allows the credential manager to track the logged-on user without querying the UPM on every session setup attempt.

Brief Description of the Drawings

Fig. 1 is a functional block diagram of a computer network in which the invention may be advantageously employed;

Fig. 2 is a schematic illustration of protocol negotiation;

Fig. 3 illustrates usage of a database by a server to obtain user definitions;

Fig. 4 is a block diagram illustrating usage of DCE registry by a server in order to obtain user definitions;

Fig. 5 is a block diagram depicting the components and signal flow of the invention implementable in the system of Fig. 1;

Fig. 6 is a schematic illustration of the token mechanism of the invention;

Fig. 7 is a block diagram illustrating the credential manager and redirector of the invention.

Fig. 9 is a state machine employed in accordance with the invention.

Detailed Description of the Preferred Embodiment

Turning first to Fig. 1, a high level description of a network environment will first be provided in which the invention

preferably may be embodied. With reference to Fig. 1, there is depicted a pictorial representation of a data processing system 8 which may be utilized to implement a method and system of the present invention. As may be seen, data processing system 8 may include a plurality of networks, such as local area networks (LAN) 10 and 32, each of which preferably includes a plurality of individual computers 12, 12a-12c, 30, 31, 33 and 35. (Hereafter, when discussing a computer in network 32, a computer 30 will be arbitrarily referenced, although the discussion could relate to any of the computers in network 32). Computers 12 and 30 may be implemented utilizing any suitable computer such as the IBM Personal System/2 (also called a "PS/2") computer or an IBM RISC SYSTEM/6000 computer workstation, both product of International Business Machines corporation, located in Armonk, New York. "RISC SYSTEM/6000" is a trademark of International Business Machines Corporation, "Personal System/2" and "PS/2" are registered trademarks of International Business Machines Corporation. Of course, those skilled in the art will appreciate that a plurality of intelligent work stations (IWS) coupled to a host processor may be utilized for each such network.

As is common in such data processing systems, each individual computer may be coupled to a storage device 14 and/or a printer/output device 16. One or more such storage devices 14 may be utilized, in accordance with the method of the present invention, to store objects, such as documents, resource objects, or executable code, which may be periodically accessed by any user within data processing system 8. In a manner well known in the prior art, each such object stored within a storage device 14 may be freely interchanged throughout data processing system 8 by transferring an object to a user at an individual computer 12 or 30, for example.

Still referring to Fig. 1, it may be seen that data processing system 8 also may include multiple mainframe computers, such as mainframe computer 18, which may be preferably coupled to LAN 10 by means of communications link 22. Mainframe computer 18 may be implemented utilizing an Enterprise Systems Architecture/370 (also called an "ESA/370") or an Enterprise Systems Architecture/390 (also called an "ESA/390") computer available from IBM. Depending on the application a mid-range computer, such as an Application System/400 (also called an "AS/400"), may be employed. "Enterprise Systems Architecture /370", "ESA/370", "Enterprise Systems Architecture/370", and "ESA/390" are trademarks of IBM; "Application System /400" and "AS/400" are registered trademarks of IBM; "Application System/400" and "AS/400" are registered trademarks of IBM. Mainframe computer 18 also may be coupled to a storage device 20 which may serve as remote storage for LAN 10. Similarly, LAN 10 may be coupled via communications link 24 through a subsystem control unit/communications controller 26 and communications link 34 to a gateway server 28. Gateway server 28 is preferably an individual computer or IWS which serves to link LAN 32 to LAN 10.

As discussed above with respect to LAN 32 and LAN 10, objects may be stored within storage device 20 and controlled by mainframe computer 18, as Resource Manager or File System Manager for the stored objects. Of course, those skilled in the art will appreciate that mainframe computer 18 may be located a great geographic distance from LAN 10 and similarly LAN 10 may be located a substantial distance from LAN 32. For example, LAN 32 may be located in California while LAN 10 may be located within Texas and mainframe computer 18 may be located in New York.

A preferred embodiment of the present invention may be incorporated within various computers depicted within data processing system 8.

In the DSS protocol, which is part of DCE, the client 100, Fig. 2, will request a ticket from the registry 122, Fig. 4, which may then be passed to the server 102. With respect to some applications, they will issue a NetUse such as that shown at 124, Fig. 7 to the redirector 116 which will kick off the protocol - essentially a user-issued command triggering the client 100 to set up a session with the server 102. In response to this NetUse, the redirector 116, then issues server management blocks (SMBs) according to the SMB communication protocol of X/Open in order to effect the negotiation of protocol and session setup. In accordance with the invention, however, in LAN servers utilizing a generic security subsystem (GSS) component of DCE, 126, Fig. 7, and a redirector such as that shown at 116, Fig. 7, as previously noted, a problem is presented of providing a mechanism for conveying requests through a credential manager 128, Fig. 8 to the GSS 126. In order to effect this mechanism, a state machine, Fig. 8, is defined for the credential manager 128 because there are commands interchanged between the credential manager and redirector required for setting up a session. The operation of this state machine will be hereinafter discussed with reference to Fig. 8 in more detail.

It will be recalled that the SMB defined by the X/Open protocol is essentially a free-form security extension which provides the concept of packages which are a mechanism employed to authenticate users. It is a significant feature of the invention that a unique such package is defined in the implementation of the invention which will provide for passing of tokens such as 130, Fig. 7. Referring further to Fig. 7, this token 130 will be seen to be passed from the GSS 126 to the credential manager 128 and then to the redirector 116 (also shown in Fig. 6). It will be recalled that the redirector 116 essentially is the component of the client. The server will make a call gss_accept_context, 133, Fig. 6, in order to process this token 130 after it has been received in the GSS package. Receipt by the redirector of the token in turn will cause the server 102 to obtain a second token, 132, Fig. 6. The client 100 will then transfer this second token 132 to the credential manager 128 and then to the GSS 126, whereupon the GSS may then authenticate the server 102.

In summary, when the first token goes across the network, the client essentially has authenticated itself to the server. If it is not authenticated, the session setup terminates whereas if it is authenticated, the session setup is effected.

Because the server has already authenticated the client, the server now will issue a function call to GSS 126, and obtain a definition from GSS of the user as previously noted. In prior systems, it is important to note that, as previously described, servers maintained their own database such as that shown in Fig. 3, reference numeral 118, to obtain a user definition 120 for verifying the user. However in accordance with the invention, the GSS is not replicated for every server, and also differing security mechanisms may be provided under GSS. The DCE extensions permit the system to obtain credentials and not only is the user authenticated but according to the system, it is thereby known which server authenticated the user. GSS is employed but it is actually the Kerberos functions in DCE which are employed underneath for the authentication.

In summary, a system is herein disclosed permitting conventional LAN server workstations and servers integrated with DCE to employ their existing mechanisms in order to pass GSS DCE credentials for authentication. Although the invention is not intended to be so limited, in the specific embodiment disclosed herein, changes are made to workstations and servers operating the OS/2 (TM) operating system available from the IBM Corporation. Further details, as background, regarding a representative LAN system may be obtained from "OS/2 Lan Server, Programming Guide and Reference", copyright IBM Corporation, S10H-9687-00, 1994, which is incorporated herein by reference. However, the aforementioned concept may be extended to stations and servers executing other operating systems as well.

In the OS/2 embodiment, the modifications to existing Lan server products will now cause the second bit of the smb_secmode field in the NP response to be turned on. The server will then wait for the previously described SMBsecpkgX or SMBsesssetupX request. The former, of course, will permit the user and server to exchange GSS tokens and mutually authenticate, and is defined in "PROTOCOLS FOR X/OPEN PC INTERWORKING: SMB VERSION 2", Section 11.2, available from the X/Open Corporation. This function permits a server to select from multiple packages.

The SMBsesssetupX following an SMBsecpkgX request may have a zero length smb_apasswd because authentication has already occurred, and any contents therein will thus be ignored. If no SMBsecpkgX request is received, or no known package was included in the SMBsecpkgX request and received, the smb_apasswd field must contain a valid password to allow the server to authenticate the user. In this case, the server must obtain the credentials for the user.

In accordance with the implementation of the invention herein described, changes must be provided to the Negotiate Protocol (NP) as follows. A Set Flag will be made to enable the secpkgx (bit number 2 in the secmode field as previously described). Still further, a new srvhueristic bit will be provided which will determine whether or not the server will support legacy clients. If legacy support is turned off, then the server will not offer the set of legacy protocols when negotiating. This will prevent the less-secure legacy clients from connection.

Also as previously noted, a new protocol level is defined which, in the specific implementation under consideration, provides that a string LSE 10 flow on the wire. In order to obtain tickets for cross-cell servers, the NP response will change to include the server's cell name and its length. The cell name will be after the domain name and will be used by the Credential Manager 128, Fig. 5, when obtaining the security context. The cell name is required for cross-cell authentication but will only be sent when negotiation results in the LSE 10 string.

Also as previously noted, secpkgX changes will be required. As noted, this function is defined in "PROTOCOLS FOR X/OPEN PC INTERWORKING: SMB VERSION 2", Section 11.2 available from X/Open. This format will be employed in the present embodiment herein disclosed, with the specific information being defined for the particular LAN server which is employed, such as the LS 4.0E available from the IBM Corporation. For the SMB_pkglist structure, the SMB_pkgname will be "Lan Server 4.0E GSS/DCE Token" which, as previously noted, will be the only package that the LS 4.0E server product will send or recognize.

In the following Table, the data structures for the aforementioned SMBsecpkgX will be defined as follows:

TABLE 1

=====			
5	Request Format:		
	BYTE	smb_com	/* value = 7E (????) */
	BYTE	smb_wct;	/* value = 4 */
	BYTE	smb_com2;	/* secondary (X) command, 0xFF = none */
	BYTE	smb_reh2;	/* reserved (must be zero) */
	WORD	smb_off2;	/* offset (from SMB hdr start) to next */
			/* cmd (@smb_wct)2 */
10	WORD	smb_pkgtype;	/* package type = 0 */
	WORD	smb_numpkge;	/* Number of Packages in list */
	WORD	smb_bcc;	/*
	struct	smb_pkglst[*];	/* package list structure. 1 package */
			/* list for LS 4.0E */
	Package List Structure (smb_pkglst) Format:		
	WORD	smb_pkgnamlen;	/* length of package name */
15	WORD	smb_pkgarglen;	/* length of the package-specific info */
	BYTE	smb_pkgname[*];	/* name of the package */
	struct	smb_pkgargs[1];	/* package-specific info for LS 4.0E */
	Package Specific Information (smb_pkgargs) Format:		
20	DWORD	smb_xp_flags;	/* Bit - If set, a reply with a GSS */
			/* token is required for mutual */
			/* authentication */
	WORD	smb_xp_TokenLen;	/* Length of GSS token */
	BYTE	smb_xp_Token[*];	/* The GSS Token containing */
			/* Authentication info */
	BYTE	smb_xp_name[*];	/* Name of user to be authenticated */
25	Response Format:		
	BYTE	smb_com	/* value = 7E */
	BYTE	smb_wct;	/* value = 4 */
	BYTE	smb_com2;	/* secondary (X) command, 0xFF = none */
	BYTE	smb_reh2;	/* reserved (must be zero) */
	WORD	smb_off2;	/* offset (from SMB hdr start) to next */
			/* cmd (@smb_wct) */
30	WORD	smb_index;	/* number of the package selected by */
			/* server. 0 for LS 4.0E */
	WORD	smb_pkgarglen;	/* length of package specific info */
	WORD	smb_bcc;	/*
	struct	smb_pkgargs[1];	/* package-specific information */
	Package Specific Information (smb_pkgargs) Format:		
35	DWORD	smb_xp_flags;	/* Bit 0, GSS tokens require another */
			/* round of exchanges. */
	BYTE	smb_xp_Token[*];	/* the GSS Token containing */
			/* authentication info */
=====			

Referring now to Fig. 5 in greater detail, the basic flow of this system is depicted therein schematically. First, the user logs on, 210, with the login context being set as system context, 211. Next, LSCredMGR function obtains credentials for a user, and the GSS credentials are created from the system context, 212, 213. This is followed by a session setup request to the server, 214. The next series of steps 215-218 represent that a context token for the Server is obtained which includes the GSS call(s) to DCE.

Continuing with Fig. 5, at step 219, the SMBsecpkg_X call is sent which contains the system context token. At this point servers obtains credentials at startup time, 220, 221 and the SMBsecpkg_X is received, 222. Next, at 223, 224, the Server will validate the user with the GSS_Accept_context function and receives a response token which includes GSS call(s) to DCE. This is followed by the server extracting EPAC from the GSS token, 225, 226. Next, the SMBsecpkg_X response is sent containing the GSS context token, 227. Also, the SMBsecpkg_X response is received, 227. As shown by steps 228-231, the Server's context token is then validated which includes GSS call(s) to DCE. Finally, as shown at reference numeral 232, the SMBsessSetup_X is sent and received.

Another aspect of the invention relates to the conventional practice of providing tokens which have a finite lifetime. When the token expires, typically the server will automatically then break connection to the client. Accordingly, some means is needed to periodically refresh the token.

Thus, in accordance with the invention, after a session is set up, the credential manager 128, Fig. 5, will determine what the remaining lifetime of a ticket is. Just before expiration, after making such determination, the credential manager 128 will thus preferably obtain a new token and transfer it to the server 102. This token may be seen represented as token 242 in Fig. 6, and will be described further with reference to the event monitoring function provided by the state

machine of Fig. 8.

The current logon status affects how the credential manager 128 manages the contexts. There are essentially four logon events which will affect the credential manager as follows.

The first, as shown in Fig. 8, is the logon function 238. The credential manager 128 must obtain the DCE system credentials. The credentials will be imported from the logon exec. Next, the logoff event 236, Fig. 8, in like manner will affect the credential manager 128. The credential manager must clear all of the session information it was maintaining for the logon user. When a logoff occurs, the RDR will close all sessions and release the DCE system credentials it is using. This event will still be needed for cleanup and state maintenance. Thirdly, a credential refresh 234 is provided for in the manner described above. This event will prevent the credential manager from transitioning into a state of expired credentials. The credential cache name will not change. If the system is already in an expired state, a new context and cache name will be acquired. The credential manager will handle both types of refreshes. Fourthly, credential expiration is provided for in the state machine, shown at reference numeral 240, Fig. 8. When the credentials expire, the credential manager 128 can no longer obtain tickets. The credential manager 128 will accordingly return an error code to the RDR when requests come in during this state. Once the user is in this state, the credentials cannot be refreshed, and a new set of credentials will be obtained by the logon exec.

Another aspect of the credential manager 128 should be noted when the client 100 is being shut down. In such event, the redirector 116 will detect this (e.g., a Net Stop function), whereupon a close command (260, Fig. 7) issued by the redirector 116 will cause the credential manager process 128 to terminate. When the systems are restarted, the redirector 116 will obviously be started upon booting. However, the credential manager 128 is not yet running until the rest of the GSS is started. Once the GSS starts, the credential manager 128 will send the token command 130 which will be held captive in the redirector 116. This thread of execution is then utilized by the redirector, which issues a connect 1 command 262. A connect 2 command, 264, holds the thread captive in the credential manager 128.

With the foregoing description in mind, additional factors in the implementation of the invention as described herein are noteworthy. It will be noted that in DCE terms, "credentials" may be thought of as Kerberos tickets or, more generically, a definition of a user and the group, the user is a member of (e.g., administrator, guest, user, etc.). Such credentials are on a per process basis typically, wherein each process is in charge of managing its own process so to speak. In accordance with the invention, however, a credential manager has thus herein been provided for the whole networking system which will manager the individual processes. Thus, in accordance with the invention, all such individual processes will have no idea that DCE credentials are operating beneath them inasmuch as the system assumes responsibility for items hereinbefore normally thought to be process-specific, such as the particular login being employed. Normally it is unique per application. However, in accordance with the invention, when applications make various calls which would otherwise have been process specific, they are now being managed at a system level basis wherein the credential manager knows what each of the processes are and sends proper credentials in order to obtain tokens.

In accordance with the invention, two software entities have essentially been merged which otherwise implement relatively dissimilar mechanisms for managing security. More specifically, the invention provided for LAN server machines to utilize their existing mechanisms in conjunction with DCE code, whereby these two entities of conventional LAN and DCE code are brought together so as to work seamlessly. It will be recalled that LAN implementations of security provide for relatively simple authentication, and one of the benefits to employing DCE authentication in accordance with the invention is because it provides a more secure environment with a more complex authentication mechanism.

In addition to the novel provision of a credential manager implementation for enabling LAN servers to operate with GSS DCE credentials, the implementation in the invention of tokens employing the SMBsecpkgX package, which is part of the X/Open specification and SMB architecture, has provided novel results. In accordance with this aspect of the invention, the novel package thereby defined includes a flag signifying mutual authentication, the hereinbefore described token, and user name which is normally obtained in a later SMB on session setup when the user is defined. Now, rather than the SMBsecpkg_X being a negotiation of the authentication protocol to use at session setups, in accordance with the invention authentication has been moved upward from session setup to the SMBsecpkgX function.

By its architectural definition, session setups are where users are authenticated. However, in accordance with the invention, authentication as noted is moved up to prior to the SMB. Thus when the system gets to a session setup, the work to effect a session setup is performed, but authentication is not required because it has already been effected. Through the novel use of a custom SMBsecpkg_X package, authentication has effectively been moved from one SMB to another. Conventional usage of this package function, however, was that when a product is sent encrypted with a session key, the feature would allow specification of different mechanisms for authentication as desired (e.g., different encryption algorithms, keys, etc.). However, the implementation of the invention, as aforesaid, facilitates moving authentication up from the session setups to the transmission of the SMBsecpkg_X package.

Claims

1. A method for improving mutual authentication during session setup with (DCE) credentials between clients and servers interconnected in a LAN server environment which does not support remote procedure calls (RPC) natively,

predefining an extension of a server management block (SMB) protocol to exchange credentials;

accessing with said server as a function of said predefined extension a generic security subsystem (GSS) through a GSS API interface defined by said DCE; and

obtaining and validating said credentials from said GSS in response to said accessing.

2. The method of Claim 1 wherein said accessing step further includes:
retrieving tokens with said clients and said server encapsulating information necessary to perform said mutual authentication.

3. The method of any previous claim wherein said extension of said SMB protocol includes:
activating a second bit in an SMB_secmode field in a negotiate protocol (NP) response.

4. The method of Claim 3 further including:

detecting with said server an SMBsecpkgX response; and

exchanging, in response to said detecting, GSS tokens between said client and said server to effect said mutual authentication.

5. The method of Claim 4 further including:
defining a GSS/DCE token package corresponding to said SMBsecpkgX response.

6. The method of Claim 5 further including:

calling with said client a GSS_initiate_sec_context function to obtain a first token to send to said server;

transferring a second token in response to said first token from said client to said GSS_initiate_sec_context function; and

returning with said GSS_initiate_sec_context function whether or not said server is authenticated.

7. The method of Claim 6 further including:

extracting said second token with said server in response to said detecting said SMBsecpkgX response;

processing said extracted token with a GSS_accept_sec_context function;

receiving with said server a GSS token to send to said client in response to a client authentication;

transferring said GSS token to said client on said SMBsecpkgX response;

extracting with said server said credentials of said user from said GSS token; and

attaching said extracted credentials to session data structures for use when said client seeks access to resources of said network.

8. The method of any previous claim wherein said server includes a redirector, and said redirector and said GSS operate at different rings, and wherein said method further includes:
establishing a credential manager process as an intermediary between said redirector and said GSS.

9. Apparatus for improving mutual authentication during session setup with distributed computing environment (DCE) credentials between clients and servers interconnected in a LAN server environment which does not support remote procedure calls (RPC) natively, comprising:

means for predefining an extension of a server management block (SMB) protocol to exchange credentials;
means for accessing with said server as a function of said predefined extension a generic security subsystem (GSS) through a GSS API interface defined by said DCE; and

means for obtaining and validating said credentials from said GSS in response to said accessing.

10. The apparatus of Claim 9 wherein said means for accessing further includes:

means for retrieving tokens with said clients and said servers encapsulating information necessary to perform said mutual authentication.

11. The apparatus of Claim 9 or 10 wherein said means for extension of said SMB protocol includes:

means for activating a second bit in an SMB_secmode field in a negotiate protocol (NP) response.

12. The apparatus of Claim 11 further including:

means for detecting with said server an SMBsecpkgX response; and

means for exchanging, in response to said detecting, GSS tokens between said client and said server to effect said mutual authentication.

13. The apparatus of Claim 12 further including:

means for defining a GSS/DCE token package corresponding to said SMBsecpkgX response.

14. The apparatus of Claim 13 further including:

means for calling with said client a GSS_initiate_sec_context function to obtain a first token to send to said server;

means for transferring a second token in response to said first token from said client to said GSS_initiate_sec_context function; and

means for returning with said GSS_initiate_sec_context function whether or not said server is authenticated.

15. The apparatus of Claim 14 further including:

means for extracting said second token with said server in response to said detecting said SMBsecpkgX response;

means for processing said extracted token with a GSS_accept_sec_context function;

means for receiving with said server a GSS token to send to said client in response to a client authentication;

means for transferring said GSS token to said client on said SMBsecpkgX response;

means for extracting with said server said credentials of said user from said GSS token; and

means for attaching said extracted credentials to session data structures for use when said client seeks access to resources of said network.

16. The apparatus of Claim 9, 10, 11, 12, 13, 14 or 15 wherein said server includes a redirector, and said redirector and said GSS operate at different rings, and wherein said apparatus further includes:

means for establishing a credential manager process as an intermediary between said redirector and said GSS.

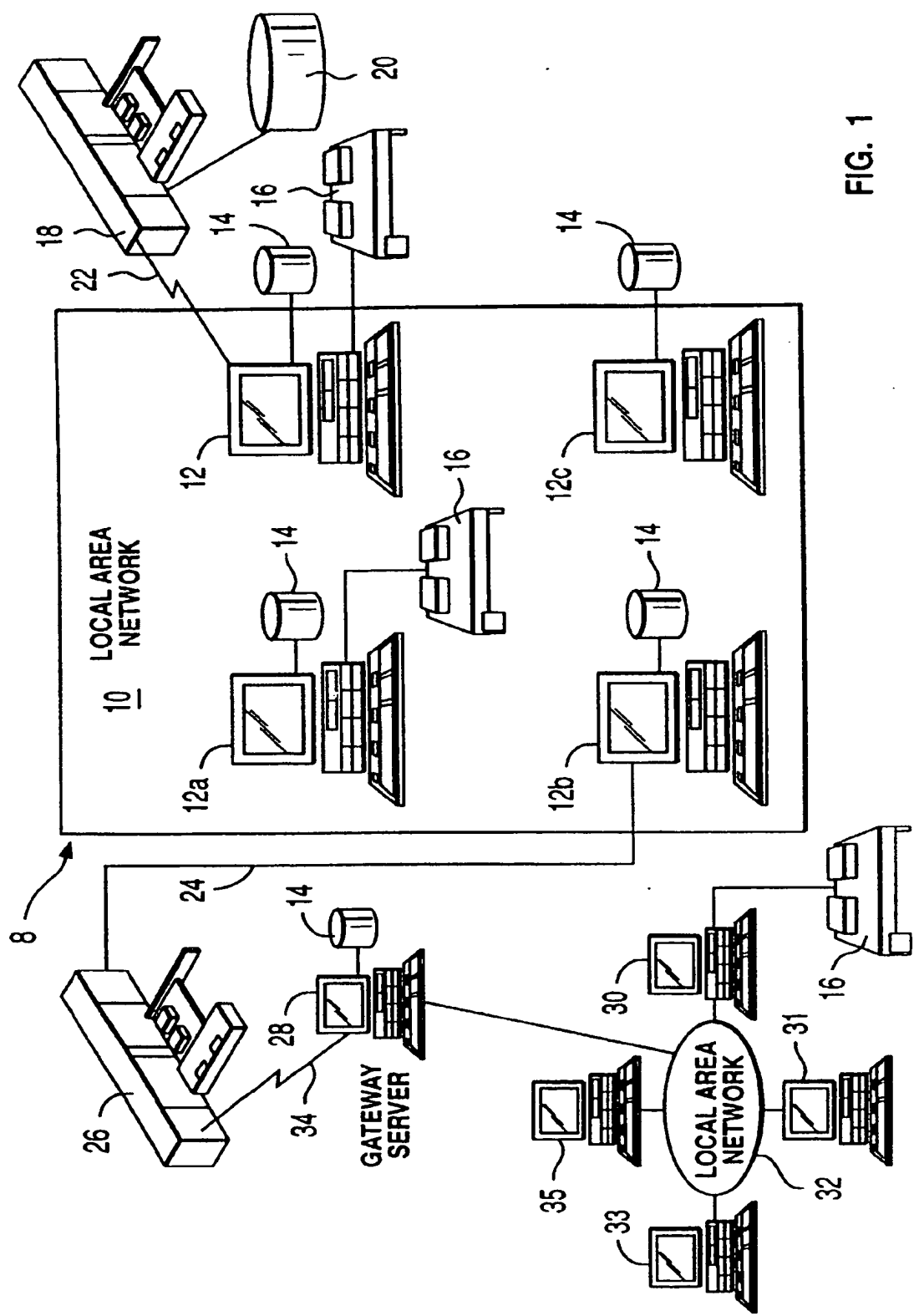


FIG. 1

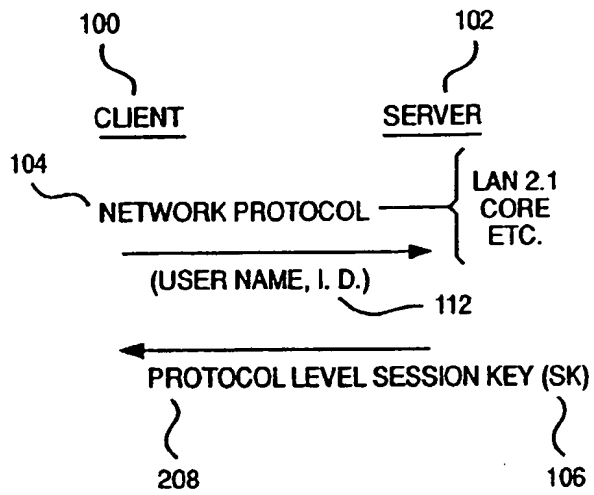


FIG. 2

FIG. 3

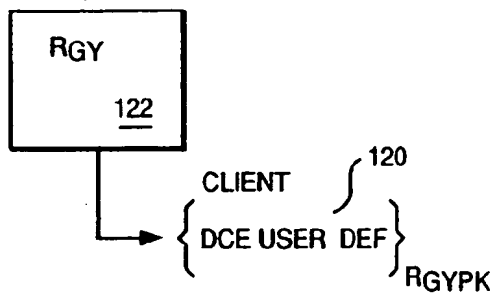
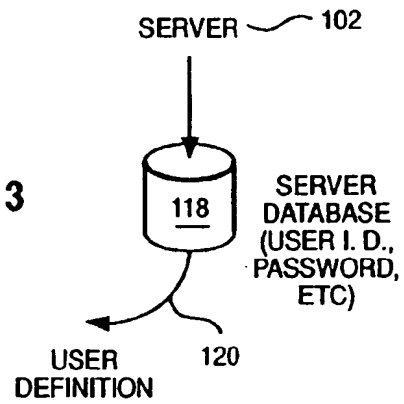


FIG. 4

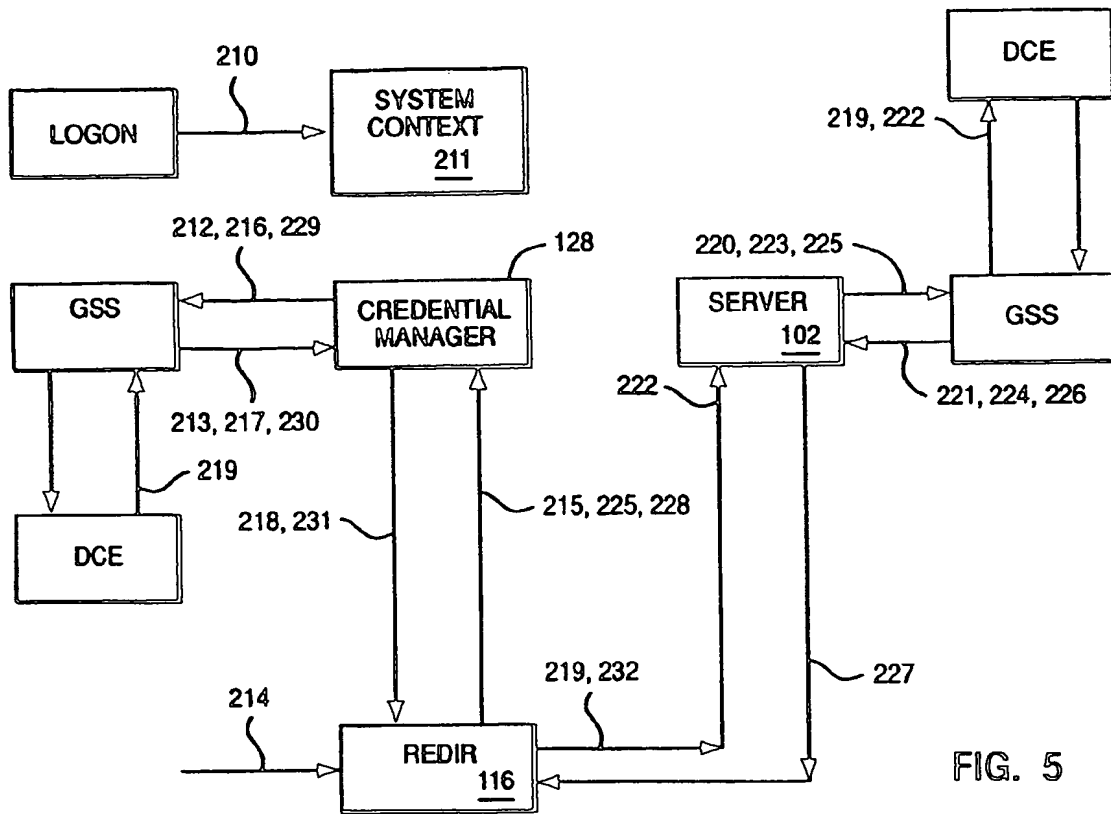


FIG. 5

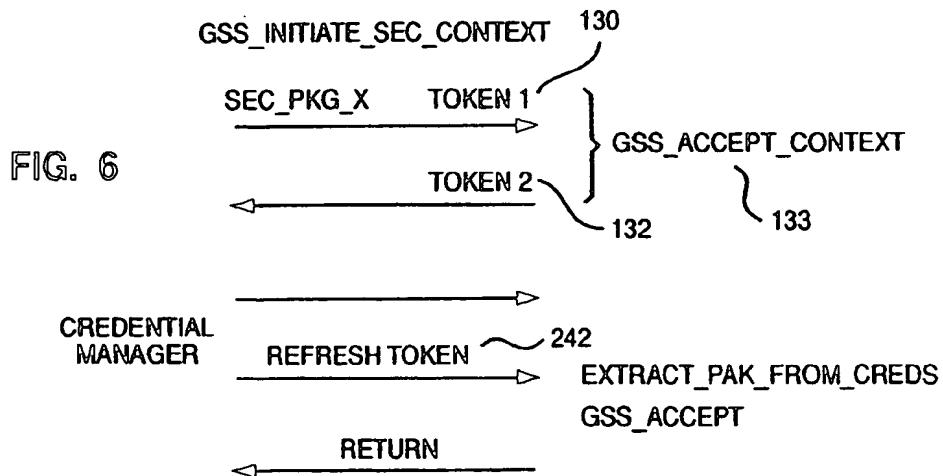


FIG. 6

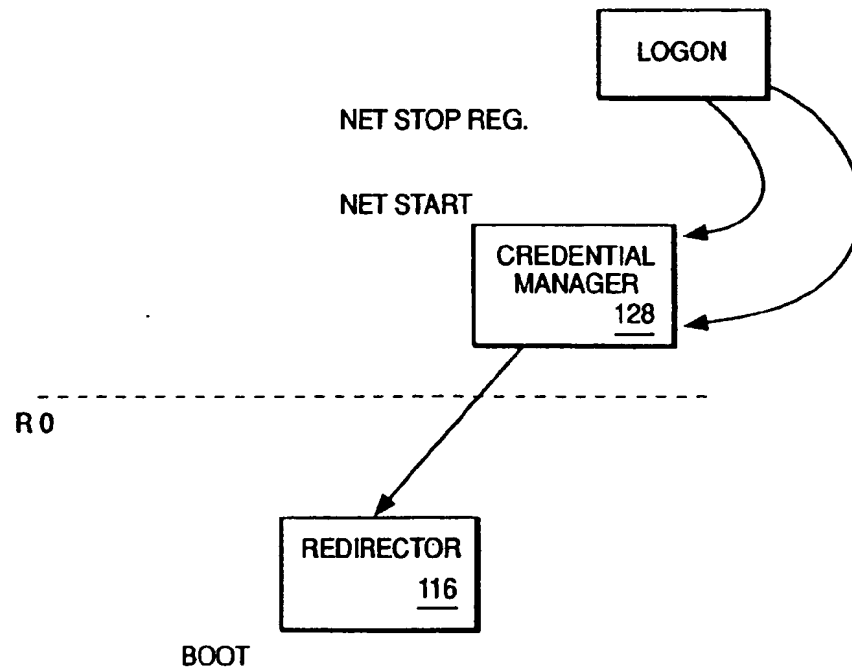
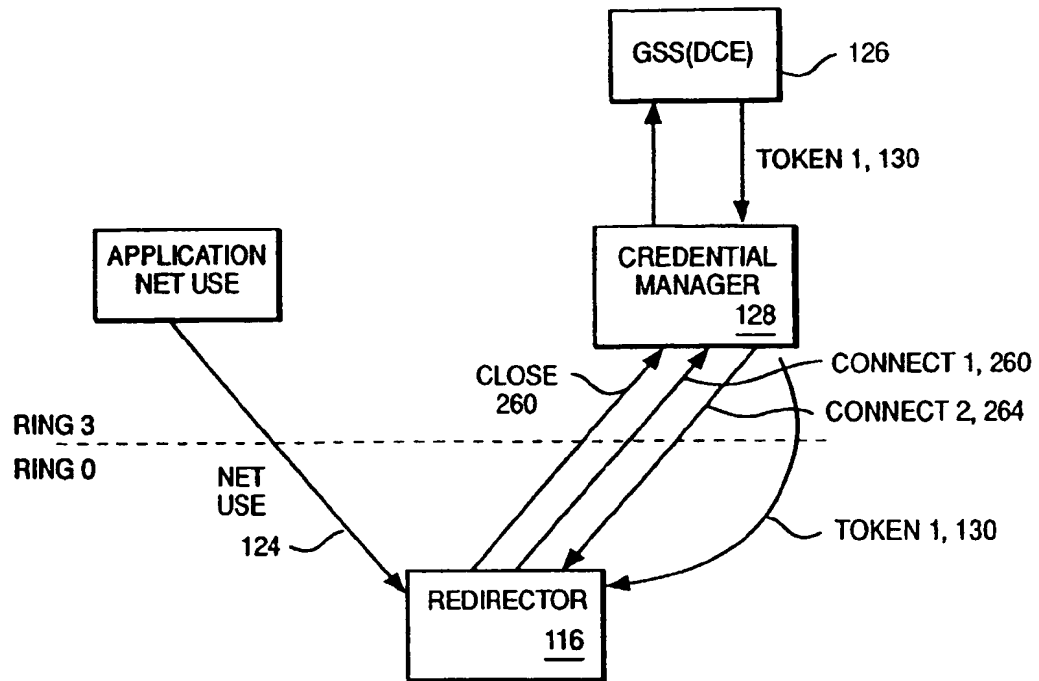


FIG. 7

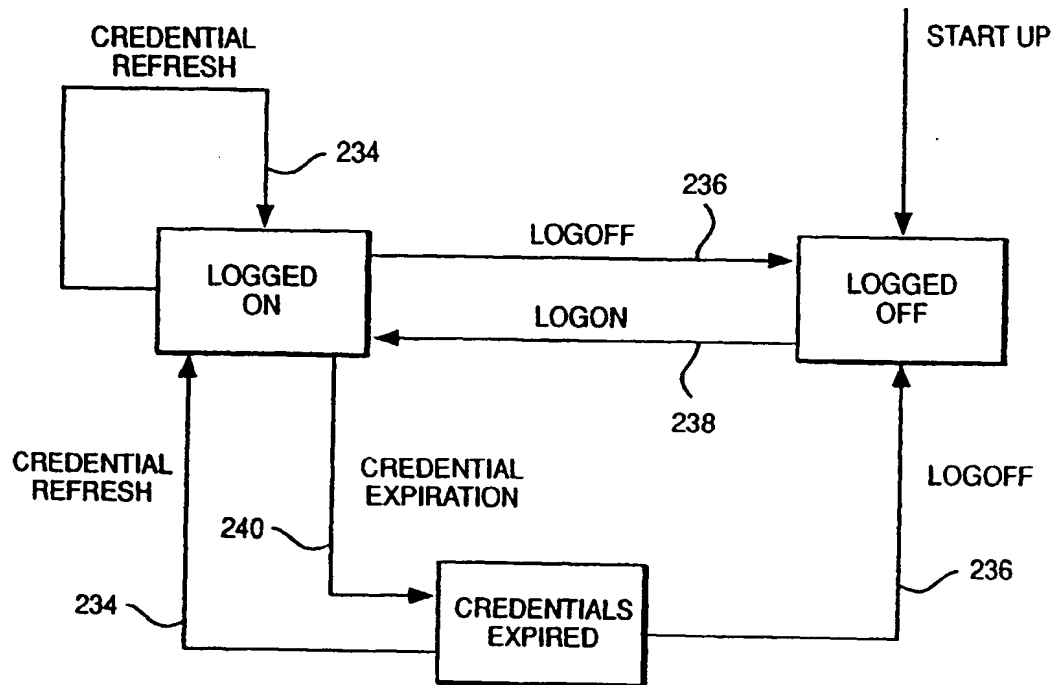


FIG. 8



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 96 30 8205

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. CL.6)
A	EP 0 398 492 A (IBM) 22 November 1990 * the whole document *	1,2,9,10	G06F1/00
A	US 5 463 625 A (YASREBI MEHRAD) 31 October 1995 * abstract; figures 1,2 * * column 2, line 36 - line 59 * * column 6, line 23 - line 46 *	1,8,9,16	
A	IBM TECHNICAL DISCLOSURE BULLETIN, vol. 33, no. 10A, March 1991, NEW YORK, US, pages 279-280, XP002026251 ANONYMOUS: "Personal Computer-Local Area Network Logon." * the whole document *	1,8,9,16	
A	IBM TECHNICAL DISCLOSURE BULLETIN, vol. 35, no. 3, August 1992, NEW YORK, US, pages 306-316, XP002026252 ANONYMOUS: "Dual Processor Boot Procedure for LAN Services." * the whole document *	1,8,9,16	TECHNICAL FIELDS SEARCHED (Int. CL.6) G06F
A	PROCEEDINGS OF THE SYMPOSIUM ON SECURITY AND PRIVACY, OAKLAND, MAY 8 - 10, 1995, no. SYMP. 16, 8 May 1995, INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, pages 50-61, XP000547690 DENG R H ET AL: "INTEGRATING SECURITY IN CORBA BASED OBJECT ARCHITECTURES" * the whole document *	1,9	
The present search report has been drawn up for all claims			
Place of search THE HAGUE		Date of completion of the search 26 February 1997	Examiner Powell, D
<p>CATEGORY OF CITED DOCUMENTS</p> <p>X : particularly relevant if taken alone V : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document</p> <p>T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document</p>			

EPF FORM 1501 (3.12.92) (P04C01)

THIS PAGE BLANK (USPTO)